Phenomenological forms of asset misappropriation fraud as the specific type of economic crime

Prof. dr Zoran S. Pavlović*
Full time Professor of Criminal law,
Chairman of the Department for Criminal Law
Faculty of Law, University of Business Academy Novi Sad,
Ombudsman of the Autonomous Province of Vojvodina,
Republic of Serbia

MA Nikola Paunović*
Research Asistant
Assistant at Ministry of Foreign Affairs
PhD Student, University of Belgrade, Faculty of law

Abstract

One of the typical phenomenological forms of economic crime in the modern world that represents a worrying threat is the asset misappropriation as the specific type of fraud. Asset misappropriation means the theft of company assets by the perpetrator for their own benefit and it can include a lot of fraud schemes committed by anyone who possesses the relevant information concerning the financial data of the target company. Bearing in mind that the consequences could affect very seriously the financial sector of the targeted company, the article deals with the phenomenological forms of this phenomenon. Precisely, since there are numerous forms, in this paper, it will be analyzed only the following phenomenological types of fraud: 1) Cash schemes; 2) Accounts receivable schemes and 3) Inventory and Fixed asset schemes. First of all, when it comes to the cash schemes, the focus will be on the forms of fraud depending on whether misappropriation of assets occurs before they are recorded in the books and records of an organization, or while assets are currently held by the organization or during the process of purchasing goods or services: a) Skimming; b) Cash larceny; and c) Fraudulent disbursements. Secondly, in the context of accounts receivable schemes, the attention will be dedicated to the following types of fraud: a) Lapping; b) Fictitious receivables. Moreover, regarding the inventory and fixed asset schemes the analysis will have consisted of the following types of fraud: 1) Simple larceny; 2) Asset requisition and transfers; 3) Purchasing and receiving schemes; and 4) False shipments of inventory. Finally, concerning the fixed asset schemes the article deals with: 1) Misappropriation of assets; 2) Recognition of fictitious assets; 3) Misrepresentation of asset value and 4) Capitalisation of non-asset expenses. In concluding remarks, it is noted that the advancement of the application of a proactive approach should be the main objective in combating the analyzed type of fraud in order to detect the asset misappropriation schemes in a timely manner.

Keywords: *phenomenology, asset misappropriation, fraud, economic crime.*

* Contact: zoran.pav@hotmail.com.
* Contact: dzoni925@gmail.com.

I. Introduction

Fraud represents widespread issue within organizations and remains a significant and high-cost problem for nearly every type of organization everywhere in the world. Bearing in mind enlarged competitive markets, rapid developments in technology and periods of economic crisis, the risks of fraud may only be increasing. Although there is no worldwide accepted definition of fraud, it could be mentioned that it essentially involves using deception to make a personal financial gain for oneself and/or create an economic loss or damage for another[1]. Since various forms of fraud are occurring at uncontrollable levels nowadays fraud has received comprehensive attention in the scientific discussions and in public actions as well. In a general sense, fraud can be committed internally or externally from a company by employees, customers, vendors and other parties. When it comes to the internal fraud, it should be noted that it usually occurs within an organization and is committed by employees, while the external fraud is perpetrated by outsiders meaning that the suspect is not an employee, manager, officer, or owner of the victim company, thereby covering a broad range of schemes, from vendor and customer frauds that attack businesses to traditional consumer frauds and confidence schemes[2]. Furthermore, fraud can be committed knowingly by a consumer (first-party fraud), or consumers can be victimized by fraudsters operating within financial institutions or as part of criminal enterprises (third-party fraud)[3]. All in all, fraud schemes are classified into three categories: *asset misappropriation* involving, but not limited to, cash larceny, skimming, and billing schemes, *corruption* in which perpetrators misuse their authority for private gain and *fraudulent financial statements* including false presentation or concealment of facts concerning the organization's financial statements[4].

Asset misappropriation means the theft of company assets, including monetary assets, cash supplies or equipment, by company directors, others in fiduciary positions or an employee for their own gain[5]. Therefore, it should be noted that asset misappropriation includes stealing an asset of a company for personal use at the corporation's expense or misuse of resources accompanied by false or deceptive records or documents to conceal the theft[6]. Asset misappropriation frauds are generally divided into two main categories: 1) *the theft of cash* and 2) *the theft of non-cash* assets. Misappropriation of assets, concerning the theft of cash, may occur under different circumstances involving the following: 1) before assets are recorded in the books and registers of an organization (e.g. *skimming*), 2) during assets are conducted by the

---

[1] Chartered Institute of Management Accountants, *Fraud risk management*, pp. 5-7, 2009, https://www.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf, accessed on 11.5.2019.

[2] Association of Certified Fraud Examiners-ACFE, *Introduction to Fraud Examination*, Association of Certified Fraud Examiners", Austin 2017, p. 75.

[3] T., Gates, K., Jacob, „Payments Fraud: Perception Versus Reality", *Economic Perspectives*, No. 1/2009, p. 7.

[4] M., Bekiaris, G., Papachristou, „*Corporate and accounting fraud: types, causes and fraudster's business profile"*, Corporate Ownership & Control, Vol. 15, No.1/2017, p. 468.

[5] K., Bussmann, *Economic crime: people, culture & controls*. PricewaterhouseCoopers, London, 2008, p. 8.

[6] R., Kassem „Detecting asset misappropriation: a framework for external auditors" *International Journal of Accounting, Auditing and Performance Evaluation*, Vol. 10, No. 1/2014, p. 3.

organization (e.g. *cash larceny*), or 3) at the time of purchasing goods or services (e.g. *billing, expense reimbursement or payroll schemes*)[7]. Finally, non-cash misappropriation of assets involves the schemes where perpetrator steal or misuse the non-cash assets of an organization, such as inventory or equipment, for own material gain[8]. In the following lines, the focus will be only to different types of internal fraud unified under the term of asset misappropriation.

II. Phenomenological forms of the asset misappropriation fraud

Majority of business-level financial crimes are consisted of stealing funds or assets over which perpetrators have control[9]. In that sense, the most common form of economic fraud is the misappropriation of assets, in which an employee, executive or owner of a company by taking advantage of his or her position steals a company's cash or non-cash assets from an organization for own personal use and gain. Therefore, it is worth mentioning that asset misappropriation falls under occupational fraud also known as the workplace, internal or employee fraud[10]. The above stated definition is pretty extensive since the majority of occupational types of theft could potentially be incorporated under the term of asset misappropriation fraud[11]. For that reason, in this paper it will be only analyzed the following phenomenological forms of asset misappropriation fraud: 1) Cash schemes, including: a) Skimming; b) Cash larceny; c) Fraudulent disbursements; 2) Accounts receivable schemes, involving: a) Lapping; b) Fictitious receivables; as well as 3) Inventory and Fixed asset schemes[12].

III. Cash schemes

1. Skimming

Skimming is known as an „*off-book*" fraud since the money is stolen before it is recorded in the books. Precisely, skimming occurs at any point where and any time when assets enter to company business, thereby anyone who deals with the process of receiving funds may be in a position to skim money (e.g. salespersons who receive assets directly from customers). In that regard, it should be pointed out that many skimming fraud schemes are committed by employees whose duties include receiving

---

[7] C., Albrecht, M., Kranacher S., Albrecht, *Asset Misappropriation Research White Paper for the Institute for Fraud Prevention*, 2010, pp. 1-2, https://www.researchgate.net/publication/242597392_Asset_Misappropriation_Research_White_Paper_for_the_Institute_for_Fraud_Prevention, accessed on 11.5.2019.

[8] *Ibid*, pp. 3-4.

[9] P., Burgess, *The 3 most common corporate fraud schemes*, 2016, https://www.microbilt.com/news/article/here-are-the-3-most-common-corporate-fraud-schemes, accessed on 6.5.2019.

[10] D., Gordon, *Understanding the 3 types of occupational fraud*, 2019, https://www.cpacanada.ca/en/news/atwork/2019-01-10-types-of-occupational-fraud, accessed on 11.5.2019; See also E., Perdue, C. McDonald, Responding to Workplace Embezzlement and Asset Misappropriation, *Michigan Defense Quarterly*, 2010, p. 14.

[11] J., P. Kennedy, „Asset misappropriation in small businesses", *Journal of Financial Crime*, Vol. 25 No. 2/2018, p. 374.

[12] Association of Certified Fraud Examiners-ACFE, *Introduction to Fraud Examination*, Association of Certified Fraud Examiners, Austin, 2011, p. 62.

and recording customers' and donors' payments[13]. In that context, it should be emphasized that there are two main types of skimming: 1) sales skimming; and 2) receivables skimming. *Sales skimming* are especially prevalent in the cases when the perpetrator has access to incoming funds from an unexpected source, such as e.g. refunds that have not been accounted for by the victim organization, while, *receivables skimming* involve the situations when incoming receivables payments are foreseen[14]. More detailed, the skimming schemes involve the following types of fraud: 1) unrecorded sales; 2) understated sales; 3) revenue skimming and 4) skimming accounts receivable[15]. The skimming in the form of *unrecorded sales* represent those type of sales that never is documented in the company books at all and could be explained by the case of an employee in which he was selling goods and services to a customer, as well as collecting the customer's payment, but did not make any record of the sale in order to steal the money. On the other hand, in the context of *understated sale*s as the specific type of skimming, the transaction in question is registered in the accounting system, but for a lower amount than what the perpetrator exactly collected. For instance, understated sales could be understood by the example of a cashier who sold 10 combination hunting and fishing licenses at $100 each, but recorded 8 at $100 each and pocketed the $200[16]. Furthermore, the form of *revenue skimming* involves cases in which the perpetrator (e.g. an employee) accepts payment from a customer, but does not record the transaction and then pockets the money. In the case of revenue skimming, a county employee embezzled at least $84,193 over two years by skimming cash receipts collected at county parks, abusing its authority to receive, record, and deposit cash receipts[17]. By contrast, in the context of *skimming accounts receivable* form, an employee accepts payments on accounts and records that the customer made a payment on the account, but falsely records a charge to an expense account with the aim of pocketing the money[18].

2. Cash larceny

Although cash larceny and skimming are very similar forms of cash fraud schemes, there is a difference between them depending on the time when the cash is stolen. In that respect, cash larceny is the theft of money that has already recorded in the company's books, while skimming is the theft of cash that has not yet been registered in the accounting system. Therefore, the key element that differentiates skimming from cash skimming is that cash larceny is referred to the amount of stolen money that is recorded in the books while regarding the skimming it does not the matter. The most common form of committing cash larceny is through the cash register since the enormous number of transactions provides an excuse for perpetrators to manipulate with the records and steal some cash, finding his or her access as a mean to rob the

---

[13] J. Finlay, *How Cash May Be Stolen*, 2009 B, pp. 1-2, http://sectorsource.ca/sites/default/files/james_finlay_nov_2009.pdf, accessed on 11.5.2019.

[14] R., Kassem, *op. cit.,* pp. 4-5.

[15] Association of Certified Fraud Examiners-ACFE, 2011, *op. cit.,* pp. 62-63.

[16] Office of the Idaho State Controller, *Revenue Skimming*, 2017, p. 1, https://www.sco.idaho.gov/web/DSADoc.nsf/F3CA0DB6B2CD938187258136005243F4/$FILE/FFFF-June_2017.pdf, accessed on 11.5.2019.

[17] *Ibid.,* p. 2.

[18] Office of Auditor General, State of Arizona, *Fraud Alert— Skimming*, 2012, https://www.azauditor.gov/sites/default/files/Fraud_Alert_12-01.pdf, accessed on 11.5.2019.

company cash and remove transaction or understate it into the records[19]. An example of cash larceny is the case regarding a bookkeeping employee, responsible for posting donors receivable in a small nonprofit agency, which was stealing some of the cash receipts but nonetheless posting the transaction to the company's donors-receivable books, thus enabling that the amount of stolen money reaches more than $200,000. Eventually, a bank reconciliation revealed a major discrepancy between the donors-receivable details and received cash and the scheme was uncovered[20].

3. Fraudulent Disbursements

Fraudulent disbursements, as the type of „on-book frauds", are the most common form of asset misappropriation, and they occur when an employee uses his position of employment to make a payment for some inappropriate purpose. Fraudulent disbursement schemes are divided into the following types: 1) check tampering schemes; 2) register disbursement schemes; 3) billing schemes; 4) expense reimbursement schemes and 5) payroll schemes[21].

Check tampering is a type of fraudulent disbursement scheme whereby an employee either 1) prepares a fraudulent check for own benefit or 2) intercepts a check intended for a third-party and converts it to own gain. By contrast from the other fraudulent disbursement schemes, such as false billings or payroll fraud which tend to rely on false claims for payment, the perpetrator of a check tampering scheme takes physical control of a check and places false information on that instrument, forging a signature and/or an endorsement as well as altering a payee or the amount of the check. The key point is that the perpetrator places false information on a company check enabling the fraudster to illegally obtain funds from employer[22]. Furthermore, there are register disbursement schemes which represent a type of occupational fraud that is a hybrid between cash theft and fraudulent disbursements. However, since these schemes appear on the books as legitimate disbursements of funds from the cash register, they are classified as fraudulent disbursements, and therefore are very similar to cash larceny schemes. On the other side, billing schemes attack the purchasing function of an organization, causing the victim organization to buy goods or services that are non-existent, high-price or not needed by the organization. This type of scheme is accomplished in one of the following two ways, either by running a voucher for a personal purchase through the payables system, misrepresenting the nature of the purpose, claiming that the goods or services are being bought on the company's behalf, or by purchasing personal goods or services on the company's credit card or on a credit account[23].

An example of using company funds for personal use represents the case in which the perpetrator as the store manager was using some of the money orders sold in her store to pay her personal bills, including the rent on her house. The money orders were pre-numbered and are stored in the vault of the store. The missing money orders caused the cash register to be short which caused the corporate office to be suspicious, thereby

---

[19] Fraud Fighting, *Cash Larceny and its types*, Fraud Fighting, 2017, p. 1, https://fraudfighting.org/wp-content/uploads/2017/12/Cash-Larceny-and-its-Types.pdf, accessed on 6.5.2019.

[20] J. Finlay, *Fraud Schames*, 2009A, p. 3, http://sectorsource.ca/sites/default/files/james_finlay_oct_2009.pdf, accessed on 7.5.2019.

[21] Association of Certified Fraud Examiners-ACFE, 2011, *op. cit.,* p. 63.

[22] *Ibid.,* pp. 63-64.

[23] *Ibid.,* pp. 64-65.

the corporate office started investigating perpetrator's paperwork and found the money orders she used to make rent and other credit card payments were cashed by a regional manager[24]. Therefore, it should be noted that a billing scheme has three major parts: a) the creation of a false entity to receive the payments by opening a bank account in the name of the false entity, or through cashing the cheques in some other manner causing that an account cannot be traced if the fraud is discovered; b) the creation of the false invoice submitted for payment; or c) the manipulation of the payments system so that the false invoice is approved and the payment is made. How this is done will depend on the position the employee has in the business and what influence he or she can have over the payment process. To conclude, all billing schemes have one common purpose regardless of their form to get the victim to voluntarily make a payment to and record the payment as a legitimate business expense[25].

Moreover, *expense reimbursement* schemes fall into four general categories: 1) mischaracterized expense reimbursements; 2) overstated expense reimbursements; 3) fictitious expense reimbursements; 4) multiple reimbursements. This type of scheme is most commonly perpetrated by sales personnel who overstate or create fictitious expenses in areas such as client entertainment and business travel. However, sales personnel are not the only employees who commit this type of fraud since any person who is in a position to incur travel or business entertainment expenses is potentially capable of committing expense reimbursement fraud[26].

Finally, there are *Payroll schemes* which occur when an employee fraudulently generates overcompensation on his or her behalf. These schemes are similar to billing schemes in a way that the perpetrator generally produces some false document or otherwise makes a false claim for distribution of funds by his employer. In other words, while in billing schemes, the false claim typically comes in the form of a fraudulent invoice, in payroll schemes, the false claim generally occurs when the fraudster falsifies payroll records, timekeeping records or some other document concerned with the payroll function. In that regard, the most common forms of payroll fraud are: 1) ghost employee schemes; 2) falsified hours and salary; 3) commission schemes[27]. Precisely, the payroll fraud includes the following examples: a) creating a ghost employee; b) claiming hours worked that were unrelated to business; c) claiming sick leave when not really sick; d) attending to personal business instead of attending professional training[28]. In that sense, for payroll forms, the following four things must take place. Firstly, the perpetrator must fabricate all the necessary personnel and payroll records for the ghost employee (false name, address, pay rate, etc.) and enter them into the payroll system. Another method used to create a ghost is to leave a terminated employee on the payroll, creating that the terminated employee becomes the ghost. Secondly, if the ghost employee is paid by the hour, the perpetrator must submit falsified timekeeping documentation to the payroll system. Thirdly, the falsified

---

[24] C., Lehmann, *„Asset Misappropriation Schemes: Short Cases for Use in the Classroom"*, Journal of Forensic & Investigative Accounting, Vol. 7, No.2/2015, pp. 343.

[25] Association of Certified Fraud Examiners-ACFE, *Billing Schemes – Cash Frauds*, ACFE Brisbane Chapter, 2019, https://brisbaneacfe.org/library/occupational-fraud/billing-schemes-cash-frauds/, accessed on 12.5.2019.

[26] Association of Certified Fraud Examiners-ACFE, 2011, *op. cit.,* p. 65.

[27] *Ibidem.*

[28] Odgen-Weber Tech College, *Fraud prevention*, 2015, p. 2, https://www.otech.edu/site/wp-content/uploads/fraud-newsletter-02.pdf, accessed on 12.5.2019.

timekeeping information must be authorized. Lastly, the pay cheque must be cut and issued, and the perpetrator must gain access to it[29].

Since the payroll schemes are difficult to detect it is worth meaning that the potential indicators of these schemes could include the following: 1) employees with duplicate addresses and/or bank account information; 2) invalid social security or social insurance numbers; 3) employees without employee's files; 4) fluctuations in payroll expense as compared to prior periods, including inconsistencies between the level of payroll comparing with department productivity; 5) timesheets with notations in different handwriting or color; 6) extra pay stubs left over after distribution to employee; 7) changes to payroll from one pay period to the next that are unsupported or unauthorized; 8) expense reports with photocopied or altered receipts, calculation errors, and supporting documentation lacking details of expenses incurred[30]. Moreover, fraud indicators in payroll schemes might be recognized by the inconsistent overtime hours for a cost center, overtime charged during a slack period, overtime charged for employees who normally would not have overtime wages as well as budget variations for payroll by cost center[31].

An example of payroll scheme fraud is the case of a financial controller, who over the years had been progressing well in terms of promotions, and thereby decided with her spouse to purchase their dream home. However, she was stunned to find out that her long-deserved promotion was being deferred indefinitely as the result of a new responsible person for finance. For that reason, she started processing the weekly payroll, adding a new fictitious, or „ghost," employee to the payroll which is a person who is on the books but does not actually work for an organization as well as using an alias name and her own legitimate bank account to set up the new employee, believing that uncovering one ghost employee among 500 was going to be like finding a needle in haystack. Within weeks, the Payroll Administrator for details and strong checks and balances uncovered the Controller's payroll fraud scheme[32].

IV. Accounts receivable schemes

1. Lapping

In the context of skimming, it seems that concealing the fraud is the most important part of the crime, even more, important than obtaining the funds. In that sense, it is worth mentioning the method of lapping[33]. Lapping is not fraud itself. It is the method of using a new fraud to hide an old fraud, in the sense that one fraud laps over another. Before the next statement is issued, an amount needs to be credited against the original debtor to hide the theft of their receipt. For example, the money needed for debtor A's

---

[29] P., Munachewa, *Payroll Fraud*, 2015, https://www.icpak.com/wp-content/uploads/2015/09/Payroll-Fraud-Munachewa.pdf, accessed on 6.5.2019.

[30] E., Nagel, *Payroll Fraud: A Global Problem:Finding a Potential Needle in the Pay Stack*, Paytech, 2015, p. 4, http://nagel-forensics.com/wp-content/uploads/2015/07/Payroll-Fraud-A-Global-Problem-Finding-a-Potential-Needle-in-the-Pay-Stack.pdf, accessed on 12.5.2019.

[31] T. Di Napoli, *Red Flags for Fraud*, New York: State Of New York Office Of

The State Comptroller, 2010, p. 7, https://www.osc.state.ny.us/localgov/pubs/red_flags_fraud.pdf, accessed on 7.5.2019.

[32] E., Nagel*, op. cit.,* pp. 2-3.

[33] J. Finlay, 2009B, p. 2.

account is taken from a receipt from debtor B - usually a debtor who pays just before the issuance of these statements. Furthermore, the money from debtor B is recorded as being collected from debtor A, hiding the fraud with debtor A, but creating a new fraud with debtor B. At the end money from debtor C is used to solve the discrepancy with debtor B, and so on[34]. This type of scheme was described by the Missouri Court of Appeals in *State v. Brown* case. According to this Court, in the context of the implementation of lapping scheme, it is necessary that the perpetrator has access to substantial amounts of cash and also is able to arrange the credit of payments made by checks to cover the misappropriated cash. In other words, lapping is an operation recognized in accounting circles as a sophisticated type of embezzlement in the form of accepting checks and failing to account for the receipt thereof in the books. However, to make the books balance, the cash should be removed in an amount equal to the face value of the checks received. Since no record has been made of the checks having been received, there is no apparent loss when the checks are used to replace the same amount of cash in the bank deposit[35].

2. Fictitious receivables

Fictitious receivables accounts are usually set up to disguise fictitious sales. Once a sale is booked, the corresponding journal entry is to a receivable that is never collected and eventually written-off[36]. Although, accounts receivable frauds start with the basics of skimming and lapping more advanced accounts receivable frauds include *account identity theft*. With account identity theft, the perpetrator sets up a bank account in a name similar to that of the victim and then steals checks intended for the victim and deposits them in the criminal's bank account in order to withdraw the funds or wire out of the account. Furthermore, there are *reaging receivables* which represents a fraud perpetrated by management when the receivables are being used for collateral for a loan. It is also done when fake sales have been entered into the accounting system in order to conceal the fact that a payment has not been made. The reaging of receivables involves creating a new receivable and using the funds to pay off an aged receivable. Finally, there are receivables *dumping* which occurs when an employee, who normally has a connection with a collection company, writes off a collectable receivable and sends it out for collection. The collection company usually gets a third of the collection and the employee either has an undisclosed interest in the collection company or is receiving a kickback from the collection company[37]. Management engaging in fraud will have two choices if intends that such frauds are not to be revealed: to intervene in the confirmation process so that phony responses can be sent to the auditors or to create journal entries that effectively move the fictitious receivables into other balance sheet accounts that will not be subject to the same level of audit scrutiny. Regarding the arrangements designed to interfere with the auditors' attempts to confirm receivables, it should be noted that this avenue commonly requires that allies of the perpetrator serve as would-be customers, who will respond favorably to the auditors' inquiries regarding

---

[34] *Ibid.,* p. 3.

[35] D., Studler, D., Malcomb, *Stealing – Back To The Basics*, Fidelity Law Association New Jersey, 2008, p. 11,
https://sdccpa.com/wp-content/uploads/2013/09/STEALING_BACK_TO_BASICS.pdf,
Retrived from 12.5.2019.

[36] Association of Certified Fraud Examiners-ACFE, 2011, *op. cit.,* p. 66.

[37] R., Minniti, *Fraud Review*, CCH Publications, Riverwoods, 2019, p. 14-15.

amounts ostensibly owed to the company. The other way, by which wholly fraudulent sales can be disguised and hidden from auditors, requires the corresponding amounts recorded as receivables be eliminated from the books before accounts are selected for confirmation. For example, receivables balances may be eliminated by means of recording fictitious returns or, more often, allowances, which are then explained as being non-cash credits to calm victimized customers[38].

V. Inventory fraud and fixed asset schemes

Inventory fraud schemes could be broken down into the following types: 1) misappropriating inventory for personal use, 2) stealing inventory and 3) theft of scrap proceeds. Phenomenological forms of inventory fraud, *misappropriating inventory for personal use* means that the inventory is being stolen for personal use under the excuse that it is being borrowed. By contrast, the inventory fraud type, *stealing inventory* involves situations when inventory is stolen for sale to outsiders, e. g. to unknowing purchasers or to co-conspirators[39]. Precisely, *inventory theft* is typically manifested by one of the following four methods: 1) simple larceny; 2) asset requisition and transfers; 3) purchasing and receiving scheme and 4) false shipments of inventory. *Simple larceny* scheme is comprised of acts in which an employee steals the company assets without any attempt to conceal it in the books. The examples of this scheme may include the following: a) theft of parts, materials, or tools used at workplaces; b) entering company premises during closed hours and stealing inventory; c) setting aside goods intended for delivery to customers or setting aside excess merchandise received. During the scheme of *asset requisition and transfers,* perpetrator moves the asset from one location to another in order to steal the inventory e.g. by requesting more material than is needed in order to steal the excess or convert it to personal gain. Furthermore, *purchasing and receiving* fraud schemes means falsifying incoming shipment records to cover up a theft and it could be perpetrated in the way that e. g. an employee who receives shipment stole some of the items, but marks the copy of the receiving document as a full shipment or marks the receiving shipment rejected since the quantity is below quality control standards. However, in fact, the rejected items do not return to the supplier, but instead sells. Finally, *false shipments of inventory* schemes include the situations which cause inventory to be shipped to a fictitious person as well as its accomplice or in some cases to a customer in order to cover up the false shipment[40]. To conclude, inventory theft can occur in many and varied forms. A common scheme involves collusion between delivery and receiving personnel, by signing for more items than were actually received in order to sell the difference to other parties and to split the money between the individuals. Another form of theft is the ordering of excess inventory items and then converting the excess to personal use. For example, in a case an employee of a motion picture company misappropriated $470,000 over a two-year period, by operating procedures which allowed him to arrange for outside script copying services, to receive script copies, and

[38] B., Epstein, *Fraudulent Revenue Schemes and How to Detect Them*, 2015, http://www.epsteinnach.com/commentary/fraudulent-revenue-schemes-detect/ accessed on 12.5.2019.

[39] Association of Certified Fraud Examiners-ACFE, 2011, *op. cit.,* p. 67.

[40] Lowers Risk Group, *Inventory, Shipping, & Receiving Fraud- Hidden Dangers in Every Transaction*, 2019, pp. 2-3, https://www.lowersrisk.com/files/resources/Inventory-Shipping-Receiving-Fraud.pdf, accessed on 12.5.2019.

to approve payments. In that sense, the employee set up a fictitious corporation, submitted invoices for services never rendered, and charged the production of films shot at the studio that were never produced[41].

Theft of Scrap Proceeds is a common practice in the case of the amounts which are generally insignificant to the financial statements of the company, since the scrap sales are usually not well controlled and inventory documentation is not well kept, enabling individuals to underreport the amounts received through the sales[42]. In that sense is a case of sale director, in which the investigation discovered that a significant proportion of sales invoiced to particular suppliers had been falsely created, allowing the misappropriation of inventory from the warehouse. The fraudulent sales invoices were later credited by the sales director as 'non-inventory return credits'. The inventory itself had been collected by an associate of the sales director and the sale proceeds shared between them[43]. To conclude, fraud indicators in inventory schemes may include increasing number of complaints about products or service, increase in purchasing inventory but no increase in sales, abnormal inventory shrinkage, lack of physical security over assets/inventory, charges without shipping documents, payments to vendors who are not on an approved vendor list, high volume of purchases from new vendors, purchases that bypass the normal procedures, vendors without physical addresses, vendor addresses matching employee addresses, excess inventory and inventory that is slow to turnover and purchasing agents that pick up vendor payments rather than have it mailed[44].

Fixed assets are the company's property, plant, and equipment. Often, fixed assets are the targets of employee theft and unlicensed personal use. Fixed assets that are easily removed from the premises (such as tools and computers) are especially exposed to employee theft[45]. Assets can be stolen directly or they can be inappropriately scrapped and sold for salvage, with the perpetrator keeping the proceeds. Furthermore, assets which have been fully depreciated but still have economic value to the company may be eliminated from the records and then stolen[46]. Another common type of fixed asset scheme is the unauthorized personal use of fixed assets by employees. For example, the personal use of computers or company-owned vehicles can develop into fraud or an abuse situation if the subject is not licensed[47]. There are four most common types of fixed asset fraud schemes: 1) misappropriation of assets; 2) recognition of fictitious assets; 3) misrepresentation of asset value and 4) capitalization of non-asset expenses. First of all, the *misappropriation of assets* happens when employees abuse their position to steal from the company. On the other side, *recognition of fictitious assets* involves the action of producing fake documents (such as invoices or purchase orders) to support the fraudulent accounting entries. Furthermore, *the misrepresentation of*

---

[41] C. Greene, *Focus on Employee Fraud*, 2019, https://www.mcgoverngreene.com/archives/archive_articles/Craig_Greene_Archives/Focus-Employee_Frauds-Invent.html, accessed on 5.5.2019.

[42] *Ibidem.*

[43] Price waterhouse Coopers Fraud, *A guide to its prevention,detection and investigation*, 2008, p. 9, https://www.pwc.com.au/consulting/assets/risk-controls/fraud-control-jul08.pdf, accessed on 6.5.2019.

[44] T. Di Napoli, *op. cit.,* p. 7.

[45] Association of Certified Fraud Examiners-ACFE, 2011, *op. cit.,* p. 67.

[46] B., Epstein, *Business And Accounting Fraud. Institute of Singapore Chartered Accountants*, Singapore, 2014, p. 29, https://isca.org.sg/media/775682/businessandaccountingfraud.pdf, Retrived fro accessed on 12.5.2019.

[47] Association of Certified Fraud Examiners-ACFE, 2011, *op. cit.,* p. 67.

asset value has several types of execution. First of all, fixed asset misrepresentations include the case of misclassification of assets to meet budgetary or covenants requirements. Moreover, in the case of understatement of values, the asset is depreciated at a higher rate compared to the estimated useful life of the asset. Finally, in the case of overstatement of values, the asset is recorded in the financial statements with a value higher than the value allowed by the applicable accounting framework. Lastly, *capitalization of non-asset expenses* scheme consists in capitalizing costs which do not meet the requirements for capitalization under the applicable accounting standards in order to show a stronger company's performance[48].

VI. Conclusion

Taking into consideration the fact that investigators are constantly faced with a lot of challenges concerning the detection of asset misappropriation schemes due to the continuous development of technology that creates new possibility for perpetrators to commit new phenomenological forms of this type of fraud or to improve the existing ones, it can be concluded that it is impossible to imagine all the potential forms of asset misappropriation schemes. In addition, it can be noted that this crime is characterized by a dark figure mostly due to lack of expertise and knowledge of relevant actors to identify potential situations that may indicate that there has been occurred the asset misappropriation. Accordingly, bearing in mind the complex and covert manifestations of asset misappropriation, it seems that the application of reactive investigation, after the criminal complaint is filed, cannot provide adequate results in terms of suppression of this type of crime. Therefore, the basic goal should be the improvement of the proactive approach in the police teamwork and public prosecutors' offices in order to achieve the sustainable reduction of asset misappropriation fraud schemes. In order to fulfill the above stated goal and make the highest results in combating economic crime, all relevant actors involved in investigations should be part of the relevant training program. In addition, it is necessary to strengthen the cooperation of state bodies that possess data relevant for carrying out investigations concerning asset misappropriation with the police and the prosecutor's office. Therefore, it should be added that starting from the covert manifestation of asset misappropriation schemes, only through comprehensive cooperation both at the international and national level in the field of information exchange, this crime could be detected in a timely manner and the valid evidence could be collected as well as used in criminal proceedings.

In that sense, it is necessary to conduct transnational investigations based on operational and strategic assistance that would be focused on the exchange of criminal intelligence data and coordination of joint investigation teams. Additionally, since perpetrators constantly adjust their activities to the latest technologies, it is extremely important to constantly collect data on new trends for commitment the asset misappropriation schemes. Furthermore, it is necessary for policy investigation teams to participate constantly in thematic training programs in order to develop the capacities and skills as well as to enable them to be prepared for all methods and techniques used by the perpetrators. Moreover, in terms of prevention, taking into account the complex and covert manifestations of asset misappropriation in order to combat efficiently against this criminal activity, it is necessary to apply a multinational

[48] Fraud fence, *Fixed assets: popular frauds and how to prevent them*, Fraud fence, 2016, http://fraudfence.co.uk/fixed-asset-frauds/, accessed on 6.5.2019.

coordinated approach, because it is unrealistic to expect that only one or several countries, without others, will achieve any results at the level of prevention. In that sense, it is necessary that all relevant actors work together on strengthening cooperation between the internal affairs bodies of national states and international organizations and European agencies. This is why it should be kept in mind that asset misappropriation schemes cannot be eradicated as such, but it should be aware that, by working together much more could be achieved in controlling this phenomenon.

References

1. Albrecht, C., Kranacher M., Albrecht, S. (2010). *Asset Misappropriation Research White Paper for the Institute for Fraud Prevention*, accessed on 11.5.2019. https://www.researchgate.net/publication/242597392_Asset_Misappropriation_Research_White_Paper_for_the_Institute_for_Fraud_Prevention.

2. Association of Certified Fraud Examiners-ACFE (2011). *Introduction to Fraud Examination*. Association of Certified Fraud Examiners, Austin.

3. Association of Certified Fraud Examiners-ACFE (2017). *Introduction to Fraud Examination*. Association of Certified Fraud Examiners, Austin.

4. Association of Certified Fraud Examiners-ACFE (2019). Billing Schemes – Cash Frauds, ACFE Brisbane Chapter, https://brisbaneacfe.org/library/occupational-fraud/billing-schemes-cash-frauds/, accessed on 12.5.2019.

5. Bekiaris, M., Papachristou, G. (2017). „Corporate and accounting fraud: types, causes and fraudster's business profile", *Corporate Ownership & Control*, Vol. 15, No.1.

6. Burgess, P. (2016). The 3 most common corporate fraud schemes, https://www.microbilt.com/news/article/here-are-the-3-most-common-corporate-fraud-schemes, accessed on 6.5.2019.

7. Bussmann, K. (2008). *Economic crime: people, culture & controls*. Pricewaterhouse Coopers, London.

8. Chartered Institute of Management Accountants, (2009). Fraud risk management, https://www.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf, accessed on 11.5.2019.

9. Di Napoli, T. (2010). *Red Flags for Fraud,* New York: State Of New York Office Of

10. Epstein, B., (2014). Business And Accounting Fraud. Institute of Singapore Chartered Accountants. Singapore. https://isca.org.sg/media/775682/businessandaccountingfraud.pdf, accessed on 12.5.2019.

11. Epstein, B., (2015). Fraudulent Revenue Schemes and How to Detect Them, http://www.epsteinnach.com/commentary/fraudulent-revenue-schemes-detect/, accessed on 12.5.2019.

12. Finlay, J. (2009A) Fraud Schames, http://sectorsource.ca/sites/default/files/james_finlay_oct_2009.pdf, accessed on 7.5.2019.

13. Finlay, J. (2009B) How Cash May Be Stolen, http://sectorsource.ca/sites/default/files/james_finlay_nov_2009.pdf, accessed on 11.5.2019.

14. Fraud fence (2016). Fixed assets: popular frauds and how to prevent them, Fraud fence http://fraudfence.co.uk/fixed-asset-frauds/, accessed on 6.5.2019.

15. Fraud Fighting (2017). *Cash Larceny and its types*, Fraud Fighting https://fraudfighting.org/wp-content/uploads/2017/12/Cash-Larceny-and-its-Types.pdf, accessed on 6.5.2019.

16. Gates, T., Jacob, K. (2009). „Payments Fraud: Perception Versus Reality", *Economic Perspectives*, No.1.

17. Gordon, D. (2019). Understanding the 3 types of occupational fraud, https://www.cpacanada.ca/en/news/atwork/2019-01-10-types-of-occupational-fraud, accessed on 11.5.2019.

18. Greene, C. (2019). *Focus on Employee Fraud,* https://www.mcgoverngreene.com/archives/archive_articles/Craig_Greene_Archives/Focus-Employee_Frauds-Invent.html, accessed on 5.5.2019.

19. Kassem, R. (2014). Detecting asset misappropriation: a framework for external auditors. Int. *International Journal of Accounting, Auditing and Performance Evaluation* Vol. 10, No. 1.

20. Kennedy, P. J. (2018) „Asset misappropriation in small businesses", *Journal of Financial Crime*, Vol. 25 Issue: 2, https://doi.org/10.1108/JFC-01-2017-0004, accessed on 5.5.2019.

21. Lehmann, C. (2015), „Asset Misappropriation Schemes: Short Cases for Use in the Classroom", *Journal of Forensic & Investigative Accounting*, Vol. 7, No.2.

22. Lowers Risk Group (2019). Inventory, Shipping, & Receiving Fraud- Hidden Dangers in Every Transaction, https://www.lowersrisk.com/files/resources/Inventory-Shipping-Receiving-Fraud.pdf, accessed on 12.5.2019.

23. Minniti, R. (2019). *Fraud Review.* CCH Publications, Riverwoods.

24. Munachewa, P. (2015). Payroll Fraud, https://www.icpak.com/wp-content/uploads/2015/09/Payroll-Fraud-Munachewa.pdf, accessed on 6.5.2019.

25. Nagel, E. (2015). „Payroll Fraud: A Global Problem: Finding a Potential Needle in the Pay Stack", Paytech, http://nagel-forensics.com/wp-content/uploads/2015/07/Payroll-Fraud-A-Global-Problem-Finding-a-Potential-Needle-in-the-Pay-Stack.pdf, accessed on 12.5.2019.

26. Odgen-Weber Tech College, (2015). Fraud prevention, https://www.otech.edu/site/wp-content/uploads/fraud-newsletter-02.pdf, accessed on 12.5.2019.

27. Office of Auditor General, State of Arizona, (2012). Fraud Alert— Skimming, https://www.azauditor.gov/sites/default/files/Fraud_Alert_12-01.pdf, accessed on 11.5.2019.

28. Office of the Idaho State Controller (2017). Revenue Skimming https:// www.sco.idaho.gov/web/DSADoc.nsf/F3CA0DB6B2CD938187258136005243F4/$FILE/FFFF-June_2017.pdf, accessed on 11.5.2019.

29. Perdue, E., McDonald, C. (2010). Responding to Workplace Embezzlement and Asset Misappropriation, Michigan Defense Quarterly, https://www.dickinsonwright.com/~/media/Files/News/2011/01/Responding%20to%20Workplace%20Embezzlement%20and%20Asset%20M__/Files/MDTCWin11_McDonald_mil_pdf/FileAttachment/MDTCWin11_McDonald_mil_pdf.pdf, accessed on 12.5.2019.

30. Price waterhouse Coopers (2008). Fraud, A guide to its prevention, detection and investigation, https://www.pwc.com.au/consulting/assets/risk-controls/fraud-control-jul08.pdf, accessed on 6.5.2019.

31. Studler, D., Malcomb, D. (2008). *Stealing – Back To The Basics*, Fidelity Law Association New Jersey, https://sdccpa.com/wp-content/uploads/2013/09/STEALING_BACK_TO_BASICS.pdf, accessed on 12.5.2019.

32. The State Comptroller https://www.osc.state.ny.us/localgov/pubs/red_flags_fraud.pdf, accessed on 7.5.2019.